Workgroup: Network Working Group
Internet-Draft: draft-ietf-jmap-smime-10
Published: 22 October 2021
Intended Status: Standards Track
Expires: 25 April 2022
Authors: A. Melnikov
Isode Ltd

S/MIME signature verification extension to JMAP

Abstract

This document specifies an extension to JMAP for Mail (RFC 8621) for returning S/MIME signature verification status.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 April 2022.

Table of Contents

1. Introduction

JMAP for Mail [RFC8621] is a JSON-based application protocol for synchronising email data between a client and a server.

This document describes an extension to JMAP for returning S/MIME [RFC8551] signature verification status, without requiring a JMAP client to download the signature body part and all signed body parts (when the multipart/signed media type [RFC1847] is used) or to download and decode CMS (when the application/pkcs7-mime media type (Section 3.2 of [RFC8551]) is used). The use of the extension implies the client trusts the JMAP server's S/MIME signature verification code and configuration. This extension is suitable for cases where reduction in network bandwidth and client-side code complexity outweigh security concerns about trusting the JMAP server to perform S/MIME signature verifications. One possible use case is when the same organization controls both the JMAP server and the JMAP client.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Type signatures, examples, and property descriptions in this document follow the conventions established in Section 1.1 of [RFC8620]. Data types defined in the core specification are also used in this document.

3. Addition to the capabilities object

The capabilities object is returned as part of the standard JMAP Session object; see Section 2 of [RFC8620]. Servers supporting _this_ specification MUST add a property called "urn:ietf:params:jmap:smimeverify" to the capabilities object.

The value of this property is an empty object in both the JMAP session _capabilities_ property and an account's _accountCapabilities_ property.

4. Extension for S/MIME signature verification

4.1. Extension to Email/get

[RFC8621] defines the Email/get method for retrieving message specific information. This document defines the following pseudo values in the _properties_ argument:

**smimeStatus*: If "smimeStatus" is included in the list of requested properties, it MUST be interpreted by the server as a request to return the "smimeStatus" response property.

**smimeStatusAtDelivery*: If "smimeStatusAtDelivery" is included in the list of requested properties, it MUST be interpreted by the server as a request to return the "smimeStatusAtDelivery" response property. (It is effectively the same as the "smimeStatus" value calculated at the date/time of delivery, as specified by "receivedAt".)

**smimeErrors*: If "smimeErrors" is included in the list of requested properties, it MUST be interpreted by the server as a request to return the "smimeErrors" response property.

**smimeVerifiedAt*: If "smimeVerifiedAt" is included in the list of requested properties, it MUST be interpreted by the server as a request to return the "smimeVerifiedAt" response property.

The "smimeStatus" response property is defined as follows:

smimeStatus: "String|null". null signifies that the message doesn't contain any signature. Otherwise, this property contains the S/MIME signature and certificate verification status calculated according to [RFC8551] and [RFC8550]. Possible string values of the property are listed below. Servers MAY return other values not defined below, as defined in extensions to this document. Clients MUST treat unrecognized values as "unknown" or "signed/failed". Note that the value of this property might change over time.

unknown:

S/MIME message, but it was neither signed nor encrypted. This can also be returned for a multipart/signed message which contains an unrecognized signing protocol (for example OpenPGP).

signed: S/MIME signed message, but the signature was not yet verified. Some servers might not attempt to verify a signature until a particular message is requested by the client. JMAP servers compliant with this document SHOULD attempt signature verification and return "signed/verified" or "signed/failed" instead of this signature status.

signed/verified: S/MIME signed message and the sender's signature was successfully verified, the sender matches the From header field, and the sender's certificate (and the certificate chain) is trusted for signing.

signed/failed: S/MIME signed message, but the signature failed to verify. This might be a policy related decision (message signer doesn't match the From header field), message was modified, the signer's certificate has expired or was revoked, etc.

The "smimeStatusAtDelivery" response property has the same syntax as "smimeStatus" but is calculated at the "receivedAt" date/time. Unlike "smimeStatus", the "smimeStatusAtDelivery" response property value is immutable. "smimeStatusAtDelivery" allows clients to compare the S/MIME signature verification status at delivery with the current status as returned by "smimeStatus", for example to help to answer questions like "was the signature valid at the time of delivery?".

The "smimeErrors" response property is defined as follows:

smimeErrors: "String[]|null". null signifies that the message doesn't contain any signature or that there were no errors when verifying the S/MIME signature. (I.e., this property is non null only when the corresponding "smimeStatus" response property value is "signed/failed". Note that future extensions to this document can specify other smimeStatus values that can be used with smimeErrors.) Each string in the array is a human readable description (in the language specified in the Content-Language header field, if any) of a problem with the signature, the signing certificate or the signing certificate chain. (See Section 3.8 of [RFC8620] in regards to how this is affected by the language selection.) In one example, the signing certificate might be expired and the message From email address might not correspond to any of the email addresses in the signing certificate. In another example the certificate might be expired and the JMAP server might be unable to retrieve a CRL for the certificate. In both of these cases there would be 2 elements in the array.

The "smimeVerifiedAt" response property is defined as follows:

smimeVerifiedAt: "UTCDate|null" (server-set). null signifies that the message doesn't contain any S/MIME signature or that there is a signature, but there was no attempt to verify it. In all other cases it is set to the date and time of when the S/MIME signature was most recently verified. Note that a request to fetch "smimeStatus" and/or "smimeErrors" would force this response property to be set to a non null value, if an S/MIME signature exists.

"smimeStatus" and "smimeErrors" values are calculated at the time the corresponding JMAP request was processed (but see below about result caching), not at the time when the message was generated (according to its Date header field value). In all cases "smimeVerifiedAt" is set to the time when "smimeStatus" and "smimeErrors" were last updated. As recalculating these values is expensive for the server, they MAY be cached for up to 10 minutes from the moment when they were calculated.

Example 1: Retrieval of minimal information about a message, including its From, Subject and Date header fields, as well as S/MIME signature verification status at delivery and date/time when the message was received.

```
["Email/get", {
"ids": [ "fe123u457" ],
"properties": [ "mailboxIds", "from", "subject", "date",
 "smimeStatusAtDelivery", "receivedAt" ]
}, "#1"]
```

This might result in the following response:

```
[["Email/get", {
   "accountId": "abc",
   "state": "51234123231",
   "list": [
     {
       "id": "fe123u457",
       "mailboxIds": { "f123": true },
       "from": [{"name": "Joe Bloggs", "email": "joe@bloggs.exampl
       "subject": "Dinner tonight?",
       "date": "2020-07-07T14:12:00Z",
       "smimeStatusAtDelivery": "signed/verified",
       "receivedAt": "2020-07-07T14:15:18Z"
     }
   ]
}, "#1"]]
```

Example 2: Retrieval of minimal information about a message, including its From, Subject and Date header fields, as well as the latest S/MIME signature verification status, S/MIME verification errors (if any) and when was the S/MIME signature status last verified. The response contains 2 S/MIME errors related to S/MIME signature verification.

```
["Email/get", {
"ids": [ "ag123u123" ],
"properties": [ "mailboxIds", "from", "subject", "date",
 "smimeStatus", "smimeErrors", "smimeVerifiedAt" ]
}, "#1"]
```

This might result in the following response:

```
[["Email/get", {
   "accountId": "abc",
   "state": "47234123231",
   "list": [
     {
       "id": "ag123u123",
       "mailboxIds": { "f123": true },
       "from": [{"name": "Jane Doe",
              "email": "jdoe@example.com"}],
       "subject": "Company takeover",
       "date": "2020-01-31T23:00:00Z",
       "smimeStatus": "signed/failed",
       "smimeErrors": [
         "From email address doesn't match the certificate",
         "Can't retrieve CRL from the CRL URL"],
       "smimeVerifiedAt": "2020-03-01T12:11:19Z"
     }
   ]
}, "#1"]]
```

4.1.1. "smimeStatus" response property extensibility

Future extensions to this document can specify extra allowed values for the smimeStatus response property. All values (defined in this document or in extensions to this document) MUST be in ASCII. (Note that this response property contains tokens, thus it is not subject to Internationalization or Localization).

New smimeStatus response property values defined in extensions may affect behaviour of properties such as smimeErrors response property of Email/get (see Section 4.1) or hasVerifiedSmime property of Email/query (see Section 4.2). In particular the new values can be treated similar to values defined in this document.

For example a putative JMAP extension for automatically decrypting S/MIME messages can specify two additional values, one specifying that a message is both encrypted and signed with a valid S/MIME signature and another one specifying that a message is both encrypted and signed with an invalid S/MIME signature. The former value can be treated as signed/verified (and would thus affect hasVerifiedSmime) and the latter can be treated as signed/failed (and thus can be used with smimeErrors).

4.2. Extension to Email/query

[RFC8621] defines the Email/query method for searching for messages with specific properties. This document defines the following properties of the *FilterCondition* object:

**hasSmime*: "Boolean". If "hasSmime" has the value true, only messages with "smimeStatus" other than null match the condition. If "hasSmime" has the value false, only messages with "smimeStatus" equal to null match the condition.

**hasVerifiedSmime*: "Boolean". If "hasVerifiedSmime" has the value true, only messages with "smimeStatus" equal to "signed/verified" (*), match the condition. If "hasVerifiedSmime" has the value false, only messages with "smimeStatus" not equal to "signed/verified" (*) (including the value null) match the condition.

(*) as well as "smimeStatus" values added by future extensions to this document that are explicitly specified as having similar effect to "signed/verified" as far as "hasVerifiedSmime" calculation is concerned.

5. IANA Considerations

5.1. JMAP capability registration for "smimeverify"

IANA is requested to register the "smimeverify" JMAP Capability as follows:

Capability Name: "urn:ietf:params:jmap:smimeverify"

Specification document: this document

Intended use: common

Change Controller: IETF

Security and privacy considerations: this document, Section 6

6. Security Considerations

Use of the server-side S/MIME signature verification JMAP extension requires the client to trust the server signature verification code, server configuration and its operational practices to perform S/MIME signature verification, as well as to trust that the channel between the client and the server is integrity protected. (For example, if the server is not configured with some Trust Anchors, some messages will have "signed/failed" status instead of "signed/verified".) A malicious or compromised server could return false verification status to a client. A successful verification could be conveyed to a client for a forged or altered message. A properly signed message could be signaled as having a failed signature verification or no signature at all. In the case of the latter attack, no new attack surface is presented with this extension above what malicious or compromised server could already do by stripping or tampering with the S/MIME information in the message. In the case of the former attack, client software capable of performing S/MIME signature verification could detect this attack. Local configuration of the client should determine if this client-side verification should occur. For clients without local verification capabilities, such an attack would be difficult to detect.

Integrity protection of the channel between the client and the server is provided by use of TLS, as required by JMAP specification (see Section 8.1 of [RFC8620]).

Constant recalculation of S/MIME signature status can result in a Denial-of-Service condition. For that reason, it is RECOMMENDED to cache results of signature verification for 10 minutes.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8550] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling", RFC 8550, DOI 10.17487/RFC8550, April 2019, <https://www.rfc-editor.org/info/rfc8550>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[RFC8620] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP)", RFC 8620, DOI 10.17487/RFC8620, July 2019, <https://www.rfc-editor.org/info/rfc8620>.

[RFC8621] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP) for Mail", RFC 8621, DOI 10.17487/RFC8621, August 2019, <https://www.rfc-editor.org/info/rfc8621>.

7.2. Informative References

[RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, DOI 10.17487/RFC1847, October 1995, <https://www.rfc-editor.org/info/rfc1847>.

Appendix A. Acknowledgements

This document is a product of JMAP Working Group. Special thank you to Bron Gondwana, Neil Jenkins, Murray Kucherawy, Kirsty Paine, Roman Danyliw and Peter Yee for suggestions, comments and corrections to this document.

Author's Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton
TW12 2NP
United Kingdom

Email: Alexey.Melnikov@isode.com